

White paper di Hikvision sul GDPR

Copyright

©2018 Hangzhou Hikvision Digital Technology Co., Ltd. TUTTI I DIRITTI RISERVATI.

La presente Documentazione non può essere riprodotta, tradotta, modificata o distribuita, in toto o in parte, con alcun mezzo senza il preventivo consenso scritto di Hikvision.

Marchi

HIKVISION® E gli altri marchi e loghi Hikvision sono proprietà di Hikvision in varie giurisdizioni. Gli altri marchi e loghi ivi citati sono proprietà dei rispettivi proprietari.

Declinazione di responsabilità

NELLA MISURA MASSIMA CONSENTITA DALLA LEGGE APPLICABILE, IL CONTENUTO DESCRITTO IN QUESTA DOCUMENTAZIONE VIENE FORNITO "COSÌ COM'È" E HIKVISION NON FORNISCE ALCUNA GARANZIA, ESPLICITA O IMPLICITA, INCLUSI, SENZA LIMITAZIONI, L'IDONEITÀ ALL'USO COMMERCIALE O A UNO SCOPO PARTICOLARE.

HIKVISION NON FORNISCE ALCUNA GARANZIA SULL'ACCURATEZZA DEL CONTENUTO DI QUESTA DOCUMENTAZIONE E SI RISERVA IL DIRITTO DI CORREGGERE O MODIFICARE IL CONTENUTO SENZA ULTERIORE PREAVVISO.

QUALSIASI DECISIONE BASATA O DERIVANTE DALL'UTILIZZO DI QUESTA DOCUMENTAZIONE, COME PURE LE EVENTUALI CONSEGUENZE CHE NE POSSONO DERIVARE, SARANNO SOTTO LA VOSTRA RESPONSABILITÀ.

IN CASO DI EVENTUALI CONFLITTI TRA IL PRESENTE MANUALE E LA LEGGE APPLICABILE, PREVALE QUEST'ULTIMA.

Content

Parte 1 Introduzione al GDPR	4
1.1 Che cos'è il GDPR	4
1.2 Il contesto	4
1.3 Obiettivi di GDPR	5
1.4 Impatto del GDPR	5
1.5 Cosa sono i dati personali?	5
1.6 Qual'è la differenza tra il titolare del trattamento (data controller) e il responsabile del trattamento (data processor)?	5
1.7 GDPR: linee guida in materia di videosorveglianza	7
1.8 Quali sono le sanzioni in caso di non-conformità?	8
Part 2 Impatto del GDPR nella videosorveglianza	9
2.1 Per la videosorveglianza cosa implica l'emanazione del GDPR?	9
Part 3 Dati e cybersecurity nei prodotti Hikvision	10
3.1 Autenticazione dell'identità	10
3.1.1 Password sicura	11
3.1.2 Attivazione	11
3.1.3 Blocco dell'indirizzo IP non autorizzato	11
3.1.4 Impostare livelli di autorizzazione per gli utenti	13
3.2. Accessibilità	14
3.2.1 Autorizzazione Live View su Lock Screen	14
3.2.2 Impostazione filtri indirizzo IP	15
3.2.3 Sicurezza delle porte d'accesso	16
3.2.4 ONVIF	16
3.3 Privacy	17
3.3.1 Data Encryption –stream encryption	17
3.3.2 Crittografia dati - HTTPS	18
3.3.3 Controllo accessi alla rete – 802.1X	19
3.3.4 Impostazione del tempo di conservazione delle registrazioni	19
3.3.5 Watermark	20

3.4 Monitoraggio dello stato	21
3.4.1 Gestione dei log	21
3.4.2 Gestione degli utenti online.....	21
Part 4 Sicurezza del cloud	23
4.1 Sicurezza del dispositivo	23
4.1.1 Protezione di sicurezza lato dispositivo.....	23
4.1.2 Associazione dispositivo.....	23
4.1.3 Crittografia streaming video	23
4.2 Altre garanzie di sicurezza.....	24
Appendice: alcuni punti chiave del GDPR.....	25
1. Ambito territoriale (Art.3)	25
2. Principi relativi al trattamento di dati personali (Art.5).....	25
3. Liceità del trattamento (Art.6).....	26
4. Condizioni applicabili al consenso del minore in relazione ai servizi della soc. dell'informazione (Art.8)...	27
5. Trattamento di categorie speciali di dati personali (Art.9).....	27
6. Diritti all'oblio (Art.17)	27
7. Diritto alla portabilità dei dati (Art.20)	28
8. Notifica di una violazione dei dati personali (Art.33, 34).....	28
9. Designazione del data protection officer (Art.37, 38, 39).....	28
10. Condizioni generali per l'imposizione di sanzioni amministrative (Art.83).....	29

Parte 1 Introduzione al GDPR

1.1 Che cos'è il GDPR

Il regolamento generale sulla protezione dei dati (GDPR), che è divenuto direttamente applicabile all'interno degli stati membri dell'UE il 25 maggio 2018, è il nuovo riferimento normativo europeo in materia di protezione dei dati personali. Il nuovo regolamento abroga la Direttiva 95/46 /CE (c.d. direttiva madre) sulla protezione dei dati) ed è stato varato per armonizzare le diverse leggi sulla protezione dei dati vigenti nei paesi europei, per proteggere e rafforzare il diritto alla privacy dei cittadini UE e per rimodellare le modalità di trattamento dei dati da parte delle organizzazioni nei diversi stati.

1.2 Il contesto

Dopo quattro anni di analisi e dibattito, il nuovo GDPR è stato finalmente approvato dal Parlamento Europeo il 14 aprile 2016. A partire dal 25 maggio 2018, dopo due anni di transizione, è divenuto pienamente esecutivo impattando su tutte le imprese che operano nell'Unione Europea. Il nuovo regolamento assicura maggiori diritti agli interessati (utenti), eleva il livello di protezione dei dati - privacy by design e by default - e la sicurezza dei dati personali. Richiede inoltre che le organizzazioni e le imprese si mostrino trasparenti sulle modalità di utilizzo e salvaguardia dei dati personali e siano in grado di dimostrare la propria responsabilizzazione (accountability) in merito al trattamento e alla gestione dei dati. Il regolamento contiene 99 articoli suddivisi in 11 capitoli, ed include le specifiche sui diritti degli interessati e gli obblighi dei titolari e dei responsabili del trattamento dati. Rispetto alla direttiva 95, che stabiliva dei requisiti minimi di protezione dei dati personali rispetto ai membri dell'UE, il GDPR porta diverse novità in termini di diritti degli interessati, obblighi del titolare del trattamento, norme sulla trasmissione dei dati, ecc.

Il GDPR risulta essere inoltre più inclusivo e flessibile.

1.3 Obiettivi GDPR

GDPR è stato introdotto per elevare il livello di protezione della privacy delle persone all'interno dell'UE, assicurare la protezione della riservatezza in ambito IoT (Internet of Things) e semplificare la gestione della protezione dei dati.

Obiettivi chiave dei GDPR sono:

- Rafforzare i diritti individuali ed assicurare un maggiore controllo sulle informazioni personali;
- Rafforzare le normative sulla privacy dei dati all'interno dell'UE;
- Assicurare che il trasferimento di dati personali ad una parte terza o ad un paese terzo avvenga dove esiste un'adeguata protezione. I dati devono essere protetti come all'interno dell'UE.

1.4 Impatto del GDPR

Il GDPR non si applica solo alle realtà all'interno dell'UE, ma anche a quelle al di fuori dell'UE che offrano beni o servizi a - o controllino i comportamenti dei - soggetti interessati dell'UE. Si applica quindi a tutte le società che trattano e conservano dati personali degli interessati residenti nell'Unione europea, indipendentemente dalla sede della società.

1.5 Cosa sono i dati personali?

Dati personali: qualsiasi informazione relativa ad una persona fisica identificata o identificabile (soggetto interessato). Una persona fisica identificabile è colei che può essere identificata, direttamente o indirettamente, in particolare facendo riferimento ad un identificativo come un nome, un numero, dei dati relativi all'ubicazione, un identificatore online od uno o più fattori specifici riguardanti

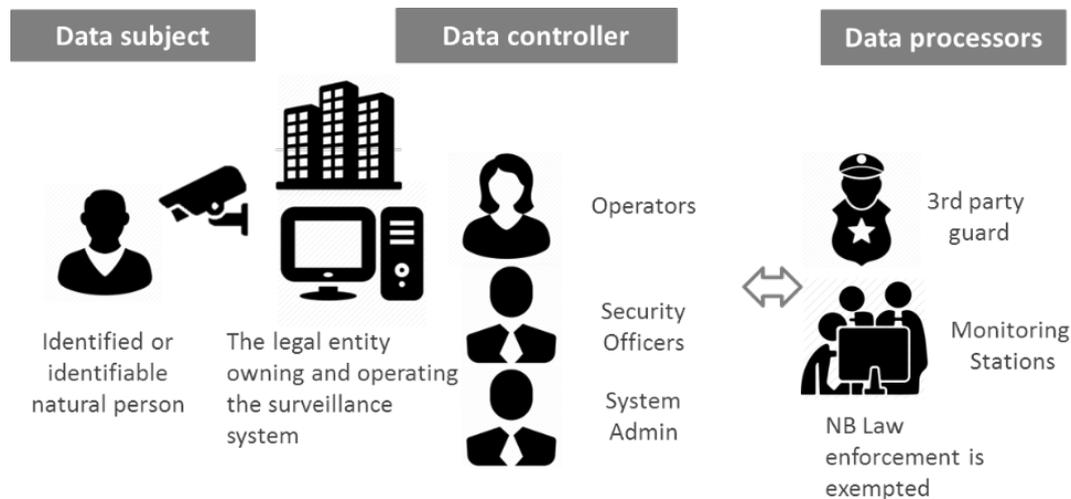
l'aspetto fisico, fisiologico, l'identità genetica, mentale, economica, culturale o sociale della persona stessa.

1.6 Qual è la differenza tra il titolare del trattamento (data controller) e il responsabile del trattamento (data processor)?

Il titolare del trattamento (data controller) è una persona - fisica o giuridica, autorità pubblica, agenzia o altro organismo - che, da sola o in collaborazione con altre, determina gli scopi, le condizioni e i mezzi del trattamento dei dati personali.

Il responsabile del trattamento (data processor) è una persona - fisica o giuridica, autorità pubblica, agenzia o altro organismo - che elabora i dati personali per conto del responsabile del trattamento.

Il rapporto che insiste tra l'interessato (data subject), il titolare del trattamento (data controller) e il responsabile del trattamento (data processor) è illustrato in figura 1.



1.7 GDPR: linee guida in materia di videosorveglianza

<p>Interessato (Data subject)</p> 	<p>Minimizzare l'acquisizione dei dati tramite:</p> <ol style="list-style-type: none"> 1. ottimizzazione della collocazione delle telecamere e del loro angolo di visuale 2. applicazione di privacy mask 	<p>Informativa agli interessati che specifici:</p> <ol style="list-style-type: none"> 1. scopi della videosorveglianza 2. chi detiene di dati (titolare/ responsabile trattamento) e a chi eventualmente viene trasmesso. 3. base giuridica del trattamento 4. politiche di conservazione dati (durata) 5. diritti dell'interessato
<p>Titolare del trattamento (Data controller)</p> 	<p>Applicare e mantenere un elevato livello di cybersecurity. Procedure di protezione dei dati personali:</p> <ol style="list-style-type: none"> 1. requisiti organizzativi 2. Data Protection Officer 3. conservare una visione generale della registrazione dei dati e flussi di processo 4. notifica della violazione dei dati entro 72 ore 	<p>Formazione del personale (obbligatoria)</p> <ol style="list-style-type: none"> 1. Formazione del personale (obbligatoria) 2. esportazione di video (incluso il mascheramento di persone di non interesse) <p>Esercizio dei diritti degli interessati</p> <ol style="list-style-type: none"> 1. limitazione degli accessi agli utenti su rigidi criteri di necessità 2. mantenere i log degli accessi utente e delle attività
<p>Responsabili del trattamento dei dati (data processor)</p>	<p>Chiunque, di terza parte, tratti dati personali per conto del titolare del trattamento è tenuto a firmare un Data Processing Agreement</p> <ol style="list-style-type: none"> 1. chiunque, di terza parte, tratti dati personali è tenuto a firmare un Data Processing Agreement 2. trasferimento di dati personali extra-UE solo a specifiche condizioni di garanzia tassativamente specificate dalla legge 3. avvalersi di una consulenza legale 	

1.8 Quali sono le sanzioni in caso di non conformità?

Violando il GDPR si può incorrere in sanzioni amministrative pecuniarie fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. Queste importanti sanzioni possono essere inflitte per le violazioni considerate più gravi, ad es. per non avere raccolto un consenso idoneo a trattare i dati o per aver violato i principi chiave della privacy by design. L'impianto sanzionatorio è organizzato su più livelli, ad es. una società può essere multata al 2% del fatturato per non avere tenuto i registri in ordine (tolto articolo 28), per non aver notificato una violazione dei dati all'autorità di vigilanza e all'interessato o per non aver effettuato l'analisi di impatto.

Parte 2 Impatto del GDPR nella videosorveglianza

2.1 Per la videosorveglianza cosa implica l'emanazione GDPR?

Il GDPR non fa esplicita menzione del settore videosorveglianza. Tuttavia il relativo mercato ne viene influenzato in maniera indiretta, dal momento che gli utenti delle soluzioni di videosorveglianza trattano e gestiscono una grande mole di dati generati dall'attività delle telecamere e dei relativi sensori.

I titolari del trattamento che gestiscono dati legati alla videosorveglianza in UE (compresi gli impianti pubblici) devono quindi prestare particolare attenzione alle disposizioni del GDPR relative all'identificazione, alla gestione e alla mitigazione dei rischi. I titolari del trattamento che gestiscono dati legati alla videosorveglianza in UE devono svolgere compiti specifici, tra i quali si annoverano la valutazione del rischio, l'assicurazione di privacy by design (fin dalla loro progettazione) dei sistemi utilizzati e lo sviluppo di segnalazioni appropriate.

In qualità di leader di mercato sul piano globale, Hikvision si impegna a proteggere i dati personali e supporta pienamente l'implementazione dei requisiti indicati dal GDPR. Hikvision ha intrapreso diverse iniziative per proteggere i dati personali nell'utilizzo dei suoi prodotti e delle sue soluzioni di sicurezza. Tra queste si annoverano la crittografia delle comunicazioni tramite algoritmi AES e protocollo HTTPS, la minimizzazione della raccolta dei dati, l'anonimizzazione dei dati, la raccolta dei dati previa autorizzazione dell'utente, la verifica della sicurezza dei dati e altro ancora.

Parte 3 Dati e cybersecurity nei prodotti Hikvision

Hikvision Security Achievement / GDPR Compliance

In qualità di leader mondiale nella produzioni di sistemi, prodotti e soluzioni di videosorveglianza caratterizzati da un elevato grado di innovazione, Hikvision si impegna ad investire ogni sforzo per fornire ai suoi clienti i prodotti e le soluzioni di sicurezza più all'avanguardia e per informare ed educare i partner e gli utenti finali in merito al tema della sicurezza dei dati.

Hikvision ha sempre attribuito grande importanza alle normative internazionali sulla sicurezza dei dati, coordinando attivamente e rispettando i più elevati standard del mercato con prodotti e sistemi di altissima qualità. Hikvision incoraggia i titolari del trattamento e i responsabili del trattamento dei dati ad aumentare i propri livelli di sicurezza seguendo queste quattro strade:

- Identità
- Accesso
- Privacy
- Stato

3.1 Autenticazione dell'identità

3.1.1 Password sicura

Hikvision raccomanda agli utenti di creare una password sicura utilizzando un minimo di 8 caratteri (incluse almeno tre tra le seguenti categorie: lettere maiuscole, lettere minuscole, numeri e caratteri speciali) per elevare la sicurezza dei prodotti utilizzare. Hikvision suggerisce inoltre agli utenti di reimpostare le password regolarmente, soprattutto in caso di sistemi ad alta sicurezza: reimpostare la password mensilmente o settimanalmente può infatti proteggere

meglio la soluzione che stanno utilizzando.

Step 1 Accendere la telecamera e connetterla alla rete

Step 2 Inserire l'indirizzo IP nella barra indirizzi del browser e cliccare Enter per accedere all'interfaccia di attivazione

Step 3 Creare una password ed inserirla nell'apposita casella

Step 4 Confermare la password

Step 5 Cliccare OK per salvare la password ed accedere all'interfaccia di visualizzazione live

3.1.2 Attivazione

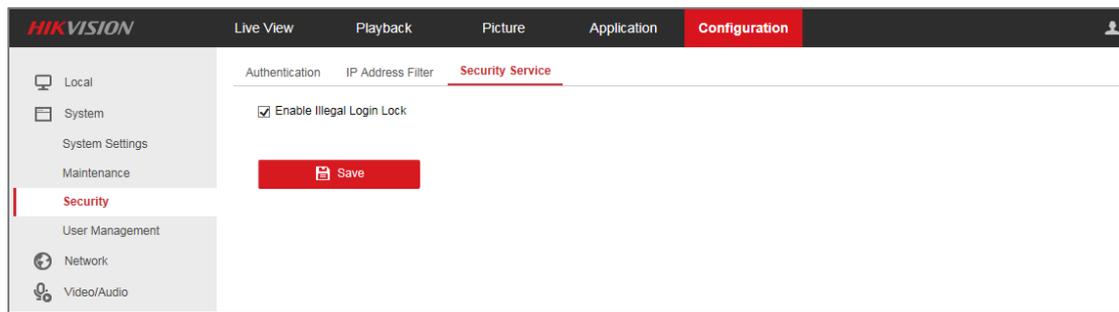
Prima di utilizzare la telecamera, è necessario attivarla impostando una password sicura.

Sono supportate l'attivazione tramite browser Web, tramite SADP e tramite software client.

3.1.3 Blocco dell'indirizzo IP non autorizzato

Per prevenire efficacemente possibili attacchi non autorizzati, l'indirizzo IP viene bloccato quando l'utente amministratore fallisce 7 tentativi di digitazione del

binomio nome utente/password (ne bastano 5 in caso di operatore/utente).



Step 1 Per accedere all'interfaccia di configurazione dei servizi di sicurezza: Configuration - System - Security - Security Service

Step 2 Selezionare la voce "Abilita blocco accessi non autorizzati". L'indirizzo IP verrà bloccato se l'utente amministratore eseguirà 7 tentativi errati di immissione nome utente/password (ne bastano 5 volte in caso di operatore/utente)

Nota: se l'indirizzo IP è bloccato, è possibile accedere nuovamente al dispositivo solo dopo 30 minuti.

3.1.4 Impostare livelli di autorizzazione per gli utenti

Per limitare l'accesso degli utenti in modo rigoroso ed impedire che dati sensibili possano essere resi disponibili ad accessi non autorizzati, Hikvision offre diversi livelli di autorizzazione per ciascun utente in modo che si possano impostare delle limitazioni sul controllo delle telecamere.

Step 1 Accedere all'interfaccia di gestione utente: Configurazione > Sistema > Gestione utenti

Step 2 Fare clic su Aggiungi per aggiungere un utente

Step 3 Immettere il nome utente, selezionare Livello e immettere la password

Nota: è possibile creare fino a 31 account utente; gli utenti di diversi livelli hanno autorizzazioni distinte predefinite. Operatore e utente sono selezionabili

Step 4 È possibile selezionare o deselezionare i permessi per ciascun nuovo utente

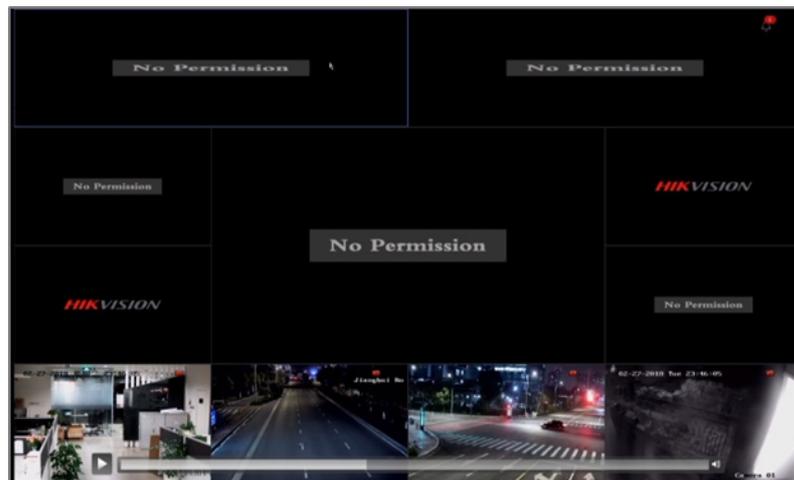
Step 5 Fare clic su OK per completare l'aggiunta dell'utente

User Management					
User List			Add	Modify	Delete
No.	User Name	Level			
1	admin	Administrator			
2	1	Operator			

3.2. Accessibilità

3.2.1 Autorizzazione alla visualizzazione Live su schermo bloccato

Questa funzione consente all'amministratore di configurare le autorizzazioni di visualizzazione live locali del dispositivo remoto. Tutti gli utenti potranno avere l'autorizzazione alla visualizzazione live locale dei canali selezionati.



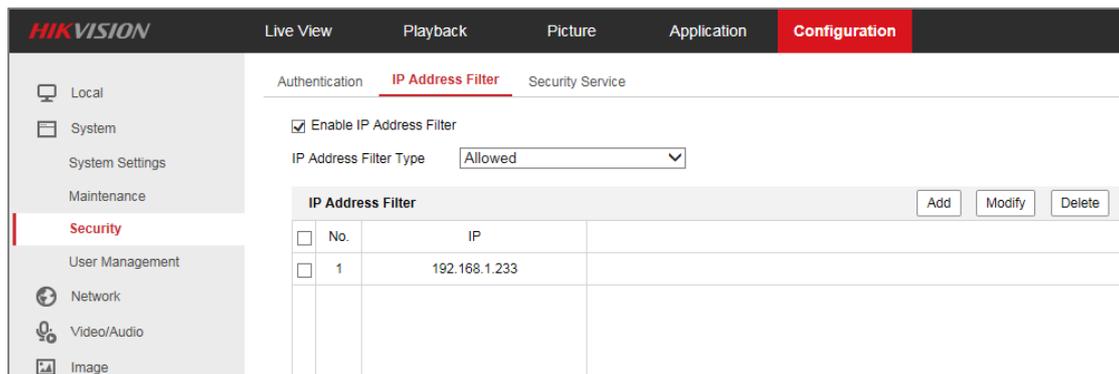
Step 1 Accedere all'interfaccia di gestione utente: Configurazione> Sistema> Gestione utenti

Step 2 Fare clic su Permessi visualizzazione live

Step 3 Selezionare il/i canale/i per abilitare la visualizzazione live sullo schermo bloccato

3.2.2 Impostazione filtri indirizzo IP

L'abilitazione del filtro IP per i client autorizzati impedisce che client non autorizzati possano accedere alle telecamere.



Step 1 Accedere all'interfaccia Filtro indirizzo IP: Configurazione> Sistema> Sicurezza> Filtro indirizzo IP

Step 2 Selezionare la casella Abilita filtro indirizzo IP

Step 3 Selezionare il tipo di filtro dell'indirizzo IP nell'elenco a tendina. Si possono selezionare Vietato e Consentito

Step 4 Selezionare il tipo di filtro dell'indirizzo IP nell'elenco a tendina. Si possono selezionare Vietato e Consentito

3.2.3 Security delle porte d'accesso

Hikvision adotta l'approccio "sicurezza di default".

La seguente funzione è stata rimossa per la sicurezza di sicurezza della rete:

- i dispositivi di Hikvision non forniscono un'interfaccia Telnet.

Le seguenti funzioni sono disabilitate di default per assicurarsi, in primo luogo, che il dispositivo non sia collegato ad una rete non sicura:

- nei dispositivi di Hikvision, l'SSH di default è disabilitato
- nei dispositivi di Hikvision, l'SNMP di default è disabilitato
- nei dispositivi di Hikvision, l'UPNP di default è disabilitato

Il multicasting è disabilitato per impedire alle telecamera i video multicasting.

Se avete necessità di attivare queste funzioni, tenete in considerazione che potrebbero comportare dei rischi per la sicurezza della rete.

3.2.4 ONVIF

La funzionalità ONVIF è disabilitata di default. Il percorso di configurazione ONVIF nel componente Web è: Configurazione > Rete > Impostazioni avanzate > Protocollo di integrazione.

Gli account utente ONVIF devono essere creati per l'applicazione ONVIF.

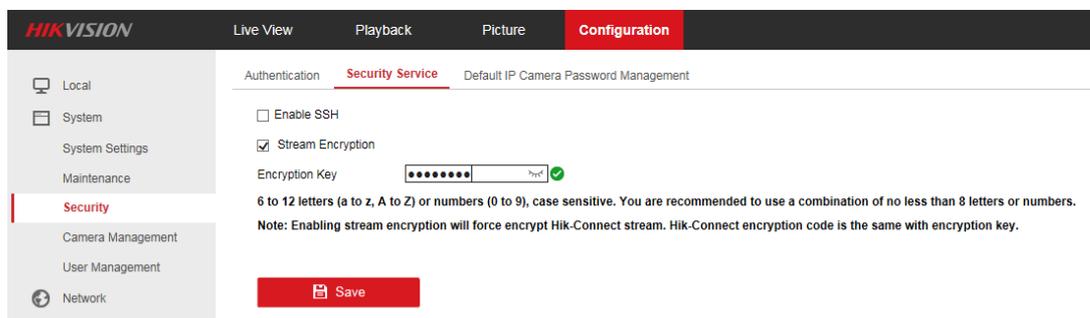
Sono selezionabili 3 livelli utente ONVIF su 17: Amministratore, Utente e Operatore, con un massimo di 32 account utente.

I Web component, iVMS-4200 e Batch Configuration sono disponibili per la configurazione ONVIF.

3.3 Privacy

3.3.1 Data Encryption –stream encryption

La crittografia del flusso consente agli amministratori di crittografare i flussi per la visualizzazione live, riproduzione, download, backup, ecc. e proteggere il trasferimento dei dati.



Step 1 Accedere all'interfaccia di configurazione del servizio di sicurezza: Configurazione > Sistema > Sicurezza > Servizio di sicurezza

Step 2 Selezionare la casella Stream Encryption e immettere la chiave di crittografia.

Nota: l'attivazione dello stream encryption forzerà la crittografia del flusso Hik-Connect. Il codice di crittografia Hik-Connect è lo stesso della chiave di crittografia.

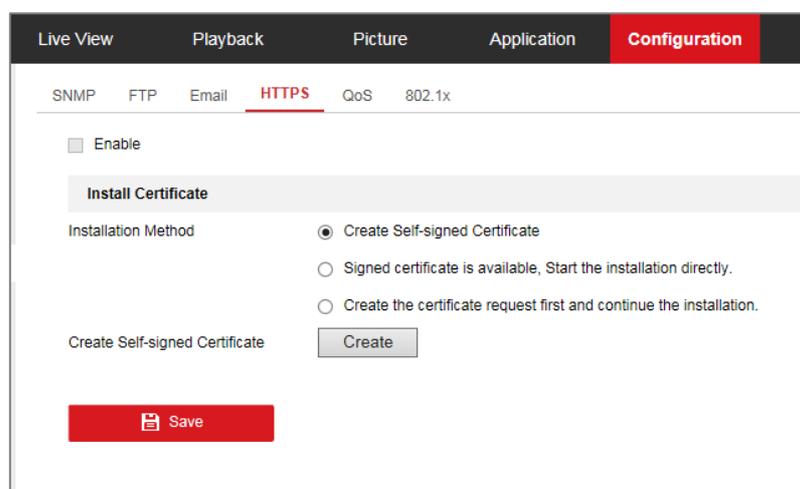
3.3.2 Crittografia dati - HTTPS

HTTPS fornisce l'autenticazione del sito Web e del relativo server Web associato, che protegge dagli attacchi "Man-in-the-middle". Effettuare le seguenti operazioni per impostare il numero di porta di HTTPS.

Ad esempio, se si imposta il numero di porta come 443 e l'indirizzo IP è 192.168.1.64, è possibile accedere al dispositivo inserendo `https://192.168.1.64:443` tramite web browser.

Step 1 Nota: l'attivazione dello stream encryption forzerà la crittografia del flusso Hik-Connect. Il codice di crittografia Hik-Connect sarà lo stesso della chiave di crittografia.

Step 2 Selezionare la casella Abilita (enable) per attivare la funzione.



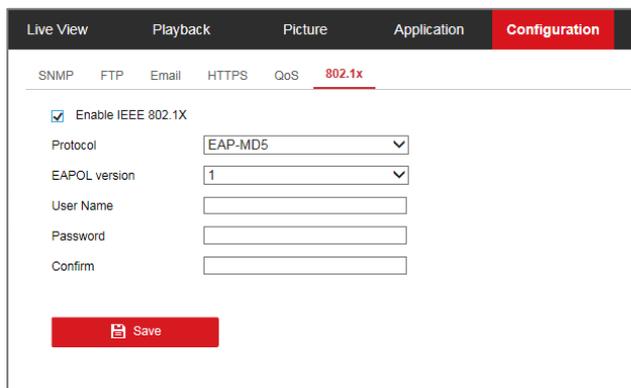
Step 3 Creare il certificato autofirmato o il certificato autorizzato.

Step 4 Le informazioni sul certificato saranno disponibili dopo aver creato e installato correttamente il certificato.

Step 5 Fare clic sul pulsante Salva per memorizzare le impostazioni.

3.3.3 Controllo accessi alla rete - 802.1X

Le telecamere di rete supportano lo standard IEEE 802.1X: quando la funzione è abilitata, i dati della telecamera sono protetti e si richiede l'autenticazione dell'utente per collegare la telecamera alla rete protetta da IEEE 802.1X. Prima di iniziare, è necessario configurare il server di autenticazione. Si prega di applicare e registrare un nome utente e una password per 802.1X nel server.



Step 1 Accedere all'interfaccia Impostazioni 802.1X, Configurazione> Rete> Impostazioni avanzate> 802.1X

Step 2 Selezionare la casella Abilita IEEE 802.1X per abilitare la funzione

Step 3 Configurare le impostazioni 802.1X, incluso Protocollo, versione EAPOL, nome utente, password e conferma

Nota: la versione EAPOL deve essere identica a quella del router o dello switch

Step 4 Immettere il nome utente e la password per accedere al server

Step 5 Fare clic su Salva per completare le impostazioni

Nota: per rendere effettive le impostazioni è necessario un riavvio

3.3.4 Impostazione del tempo di conservazione delle registrazioni

Il tempo di conservazione dei dati è il lasso di tempo nel quale un file registrato viene tenuto nell'HDD. Una volta giunto a scadenza, il file verrà eliminato. Se si imposta la scadenza su 0, il file non verrà eliminato. Il tempo di conservazione del file deve essere determinato dal titolare del trattamento quando si imposta un Requisito Operativo (OR) o gli obiettivi per l'uso del sistema TVCC e questo sarà influenzato anche dalla capacità dell'HDD.

Advanced Parameters

Record Audio:

Pre-Record:

Post-Record:

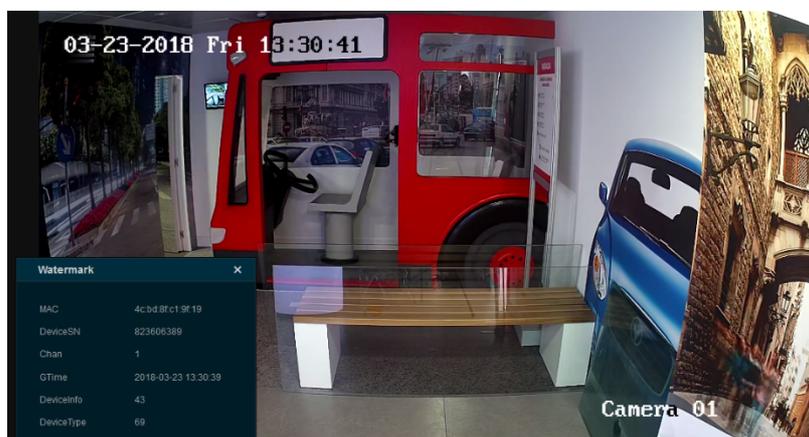
Stream Type:

Expired Time (day):

Redundant Record/Capture

3.3.5 Watermark

L'aggiunta di una marcatura nello stream video è ideale per gestire i problemi di manipolazione video. Il Watermark (filigrana elettronica) è infatti nascosta nei file originali. E' possibile visualizzare le informazioni solo con Hikvision VSPlayer.



3.4 Monitoraggio dello stato

3.4.1 Gestione dei log

Per garantire che tutte le operazioni possano essere tracciate, le operazioni eseguite, gli allarmi rilevati, le anomalie riscontrate e le informazioni della telecamera, possono essere memorizzate nel file di log. Su richiesta, è possibile esportare i file di log. Vengono forniti anche i log degli allarmi.

The screenshot shows the Hikvision web interface. The top navigation bar includes 'Live View', 'Playback', 'Picture', and 'Configuration'. The left sidebar has categories like 'Local', 'System', 'Maintenance', 'Security', 'Camera Management', 'User Management', 'Network', and 'Video/Audio'. The main content area is titled 'Upgrade & Maintenance' and 'Log'. It features search filters for 'Major Type' (All Types), 'Minor Type' (All Types), 'Start Time' (2018-03-23 00:00:00), and 'End Time' (2018-03-23 23:59:59). Below the filters is a 'Log List' table with an 'Export' button.

No.	Time	Major Type	Minor Type	Channel No.	Local/Remote User	Remote Host IP
1	2018-03-23 00:22:05	Operation	Remote: Configure Para...		admin	192.168.1.65
2	2018-03-23 00:22:05	Operation	Remote: Configure Para...		admin	192.168.1.65
3	2018-03-23 00:22:05	Operation	Remote: Configure Para...		admin	192.168.1.65
4	2018-03-23 00:22:05	Operation	Remote: Configure Para...		admin	192.168.1.65

Step 1 Accedere all'interfaccia di ricerca file di log: Configurazione > Sistema > Manutenzione > Registro

Step 2 Impostare le condizioni di ricerca file di log specificando i criteri di ricerca, inclusi il tipo principale, il tipo minore, l'ora di inizio e l'ora di fine. Fai clic su Cerca per trovare i file di log. I file corrispondenti verranno visualizzati nell'interfaccia dell'elenco file di log

3.4.2 Gestione degli utenti online

Attraverso questa interfaccia è possibile individuare gli utenti che stanno visitando il dispositivo. Le informazioni utente (es. nome utente, livello, indirizzo

IP e orario di funzionamento) sono visualizzate nella Lista utenti.

The screenshot shows the Hikvision web interface. At the top, there is a navigation bar with tabs: Live View, Playback, Picture, Application, and Configuration (which is highlighted in red). On the left side, there is a sidebar menu with categories: Local, System (containing System Settings, Maintenance, Security), User Management (highlighted in red), Network, Video/Audio, Image, Event, and Storage. The main content area is titled 'User Management' and has a sub-tab 'Online Users' (highlighted in red). Below this, there is a 'User List' table with a 'Refresh' button in the top right corner. The table has five columns: No., User Name, Level, IP Address, and User Operation Time. There is one row of data.

No.	User Name	Level	IP Address	User Operation Time
1	admin	Administrator	192.168.1.200	2018-03-23 19:52:01

Step 1 Fare clic su Aggiorna per aggiornare l'elenco

Parte 4 Sicurezza del cloud*

4.1 Sicurezza del dispositivo

4.1.1 Protezione di sicurezza lato dispositivo



4.1.2 Associazione dispositivo

- Numero di serie e autenticazione del codice di verifica
- Un solo dispositivo per un solo account

4.1.3 Crittografia streaming video

- AES-128 bit
- Richiesta codice di crittografia per il nuovo apparato che desidera collegarsi
- Codice di crittografia modificabile, controllato solo dal proprietario del dispositivo
- Crittografia End-to-end

4.2 Altre garanzie di sicurezza

- Test di sistema trimestrali dell'integrità del nostro sistema rispetto a possibili minacce alla sicurezza di terze parti
- Impostazione di una piattaforma esterna di raccolta delle vulnerabilità
- Team di R&D completamente dedicato alla sicurezza
- Utilizzo di Deep Security di Trend Micro per salvaguardare i dati

Certificazione di terze parti

- Certificazione ISO 27001

- Garanzia ai clienti

Con la certificazione ISO 27001, il cliente consolida la sua fiducia verso di noi anche lato privacy e si fidelizza, permettendoci di mantenere nel tempo la clientela e di generarne di nuova.

- SOC 2 Type 1 Report

- I Controlli dell'Organizzazione di servizio 2 sono norme rigorose progettate dall'AICPA, coperte da SSAE 16, per garantire che i fornitori di servizi tecnologici dispongano di sistemi adeguati per proteggere le informazioni e i dati dei clienti.

- Di che parla?

Sicurezza - protezione da accessi non autorizzati fisici e logici. **Disponibilità** - disponibilità del sistema per il funzionamento e l'utilizzo, come concordato.

Integrità di elaborazione - garantisce che l'elaborazione del sistema sia autorizzata, completa, accurata e tempestiva.

Riservatezza - protezione delle informazioni riservate, come concordato.

Privacy - garantisce che le informazioni personali siano raccolte, utilizzate, conservate e divulgate in conformità con l'informativa sulla privacy delle imprese, nonché sui principi di AICPA e CICA.

Appendice: alcuni punti chiave del GDPR

Riportiamo alcuni punti chiave degli articoli più rilevanti del regolamento. Per maggiori dettagli si prega di consultare la norma.

1. Ambito territoriale (Art.3)

Il presente regolamento si applica:

- 1) al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione;
- 2) al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:
 - a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato;
 - b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.
- 3) al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

2. Principi relativi al trattamento di dati personali (Art.5)

I dati personali sono:

- a) a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
- b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattate in modo che non siano incompatibili con tali finalità;
- c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
- d) esatti e, se necessario, aggiornati;
- e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
- f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Il titolare del trattamento sarà ritenuto responsabile e deve essere in grado di dimostrare la conformità a quanto sopra.

3. Liceità del trattamento (Art.6)

Il trattamento può essere considerato lecito solo se si concretizza almeno una delle seguenti condizioni:

- a) l'interessato ha prestato il consenso al trattamento dei propri dati personali per uno o più scopi specifici;
- b) b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- c) il trattamento è necessario per adempiere a un obbligo legale a cui è soggetto il titolare del trattamento;

- d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- f) f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

4. Condizioni applicabili al consenso del minore in relazione ai servizi della società dell'informazione (Art.8)

Qualora si applichi come base giuridica il consenso dell'interessato, per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale. Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni.

5. Trattamento di categorie speciali di dati personali (Art.9)

Il trattamento di dati personali è vietato se volto a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. Questo divieto non si applica se, ad esempio, l'interessato ha espresso il consenso esplicito al trattamento di tali dati personali, o il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale.

6. Diritto all'oblio (Art.17)

L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

- a. i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
- b. l'interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento;
- c. l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;
- d. i dati personali sono stati trattati illecitamente;
- e. i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
- f. i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione

7. Diritto alla portabilità dei dati (articolo 20)

L'interessato ha il diritto di ottenere in un formato strutturato i dati personali che lo riguardano, da questi forniti a un titolare del trattamento, e di trasmetterli a un altro titolare, qualora si tratti di un trattamento effettuato con mezzi automatizzati e nei casi in cui la base giuridica sia il consenso o l'esecuzione di un contratto di cui l'interessato è parte.

8. Notifica di una violazione dei dati personali (Art.33, 34)

In caso di violazione dei dati personali, il titolare del trattamento procede senza indugi e, ove possibile, entro 72 ore dalla sua conoscenza dei fatti, alla notifica della violazione all'autorità di vigilanza competente. Quando la violazione dei dati personali può comportare un rischio elevato per i diritti e le libertà delle persone fisiche interessate, il titolare del trattamento deve immediatamente comunicare anche a questi ultimi che si è verificata una violazione dei dati personali.

9. Designazione del data protection officer (Art.37, 38, 39)

Il titolare del trattamento e il responsabile del trattamento designano un data protection officer per garantire la conformità della protezione dei dati e per trattare gli aspetti più rilevanti della protezione dei dati.

10. (Condizioni generali per l'imposizione di sanzioni amministrative (articolo 83))

Le autorità hanno il potere di valutare l'entità delle sanzioni affinché risultino effettive, proporzionate e dissuasive. Il GDPR prevede due livelli massimi di sanzioni, in base alla gravità della violazione:

- a. fino a 10 000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore
- b. fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore

L'importo della sanzione è valutato sulla base di:

- 1. natura, gravità e durata dell'infrazione;
- 2. carattere intenzionale o negligente della violazione (natura dolosa o colposa);
- 3. grado di responsabilità del titolare del trattamento o del responsabile del trattamento;
- 4. precedenti violazioni da parte del titolare del trattamento o del responsabile del trattamento;
- 5. tipologia di dati personali interessati dalla violazione;
- 6. maniera in cui l'autorità di controllo ha preso conoscenza della violazione;
- 7. grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
- 8. rispetto di eventuali provvedimenti disposti nei confronti del titolare del trattamento o del responsabile del trattamento dall'autorità di controllo;
- 9. adesione ai codici di condotta approvati o ai meccanismi di certificazione approvati;
- 10. vantaggi finanziari derivanti, direttamente o indirettamente, dall'infrazione.